REMARKS

Claims 8, 10-15, and 17-18 are now pending in the application. The Examiner is respectfully requested to reconsider and withdraw the rejections in view of the amendments and remarks contained herein.

REJECTION UNDER 35 U.S.C. § 103

Claims 8, 10-15, and 17-18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Moskowitz et al. (U.S. Pat. No. 5,745,569) in view of Leighton (U.S. Pat. No. 5,949,885), further in view of Rhoades (U.S. Pat. No. 5,745,569), and yet further in view of Barton (U.S. Pat. No. 6,047,374). This rejection is respectfully traversed.

Moskowitz et al. is generally directed toward embedding active, hidden data made up of executable control code in a non-executable bit stream of media content, wherein the control code is needed by a media content delivery application to deliver the media content based on the non-executable bit stream. In particular, Moskowitz et al. is directed toward encrypting the active hidden data with a license-based key so that the user will have to provide the appropriate copyright license information to enable decryption of the active hidden data (column 6, lines 8-36). Thus, Moskowitz et al. teaches embedding active hidden data, but does not teach embedding control data.

The Examiner references '569 Abstract for "digital watermark contains licensing information interwoven with essential code resources encoded into data resources" to provide the embedded control data. Perhaps the Examiner thinks that the licensing key is embedded in the non-executable bit stream. However, the licensing information is only "interwoven" with the essential code resources in the sense that the active hidden

data is encrypted based on the licensing information. Moreover, the Examiner must agree that it is impossible for one to obtain the licensing key for decrypting the active hidden data if the licensing key is encrypted based on the licensing key along with the essential code resources. Further, even if the Examiner interprets the control code encrypted based on the licensing key as embodying both active hidden data and control data, then it remains impossible for this "control data" to be embedded orthogonal to the active hidden data while still obtaining the function in accordance with the teachings of Moskowitz et al. Thus, modifying Moskowitz et al. to arrive at active hidden data embedded orthogonal to an error correction data portion of the control data is proscribed by MPEP §2143.01 because the proposed modification would render the prior art unsatisfactory for its intended purpose. Thus, Moskowitz et al. cannot teach, suggest, or motivate active hidden data embedded orthogonal to an error correction data portion of the control data that is used to ensure the errorless extractability of the active hidden data from the embedded data stream.

Leighton et al. is generally directed toward watermarking embedding techniques to overcome averaging attacks using multiple copies of a work. In particular, Leighton et al. is directed toward embedding one or more copies of a watermark in a document at different vectors so that averaging attacks using multiple documents are less likely to destroy all watermarks in the copy. In one case, a next offset watermark is embedded orthogonal to the previous water mark upon which it is based to reduce noise. Leighton et al., however, does not teach, suggest, or motivate active hidden data embedded orthogonal to an error correction data portion of the control data that is used to ensure the errorless extractability of the active hidden data from the embedded data stream.

Rhoads et al. is generally directed toward using digital watermarks to copy protect a music with a compliant copying device. In particular, a reference count employed by the compliant device is embedded in the music as a watermark, and the count is decremented when the compliant device copies the stream and embeds a new reference count value watermark orthogonal to the previous reference count watermark. The Examiner apparently considers one instance of the embedded reference count to be active hidden data, and another instance of the embedded reference count to be control data. This view, however, is erroneous in that the reference count is not control data since it does not govern the use of active hidden data. Nor is the reference count active hidden data, since it only contains data upon which the application can act, rather than executable control code. As a result, Rhoads et al. does not teach, suggest, or motivate active hidden data embedded orthogonal to an error correction data portion of the control data that is used to ensure the errorless extractability of the active hidden data from the embedded data stream.

Barton et al. is generally directed toward using an embedded digital signature that is a reduced representation of a digital block in which it is embedded to verify that the digital block has not been modified. In particular, an error correction code is added to the digital signature after encryption and the resulting bit stream containing the encrypted signature and the correction code is embedded in the block. In one case, the bit stream is embedded in three separate locations of the image. Upon extraction of the bit stream, the bits of the error correction code are compared to obtain a final code employed to restore the digital signature to its original condition so that it can be properly decrypted (column 9, lines 8-15). However, Barton et al. does not teach,

suggest, or motivate active hidden data embedded orthogonal to an error correction data portion of the control data that is used to ensure the errorless extractability of the active hidden data from the embedded data stream.

Applicant's claimed invention is generally directed toward hiding active data made up of executable control code in a non-executable bit stream of media content, wherein the control code is needed by a media content delivery application to deliver the media content based on the non-executable bit stream. In particular, Applicant's claimed invention is directed toward embedding control data that governs the use of the active hidden data orthogonal to the active hidden data. In a preferred embodiment, the control data includes authentication data and error correction data that are also embedded orthogonally to one another to maximize detection of the three sets of information. The authentication data is checked as a prerequisite to extraction of the active hidden data. Subsequently, error correction data relating to the active hidden data is extracted and employed to ensures errorless extraction of the active hidden data from the embedded data stream. In particular, the error correction data serves as a reference for detecting and correcting errors in the active hidden data.

The differences between Applicant's claimed invention and the cited references are significant. For example, independent claims 8 and 15 recite "hidden data embedded orthogonal to an error correction data portion of the control data ... used to ensure the errorless extractability of the active hidden data from the embedded data stream". Also, dependent claim 12 recites "at least a portion of the control data as error correction data relating to the active hidden data". Further, dependent claim 13 recites "authentication data embedded orthogonal to the hidden active data and error correction

data". As a result, none of the cited references, alone or combined, teach suggest, or motivate all of the limitations of independent claims 8 and 15, or dependent claims 12 and 13. Moreover, one skilled in the art and faced with the teachings of the cited references would be required to accomplish substantial innovation to arrive at Applicant's claimed invention, which obtains several functional differences over the teachings of the cited references.

Applicant respectfully asserts that claims 8, 10-15, and 17-18 are in condition for allowance as none of the cited references teach, suggest, or motivate active hidden data embedded orthogonal to an error correction data portion of the control data that is used to ensure the errorless extractability of the active hidden data from the embedded data stream. Therefore, Applicant respectfully requests that the rejections to independent claims 8 and 15 under 35 U.S.C. § 103(a) be withdrawn, along with rejection on these grounds of all claims dependent therefrom.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt

and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: August 12, 2003

By: 
Gregory A. Stobbs
Reg. No.: 28,764

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

[JSB/kp]